

the personal data is rendered unrecognizable or beyond reconstruction.

(2) The transfer of large quantities of records containing personal data (for example, computer cards and print-outs) in bulk to a disposal activity, such as the Defense Property Disposal Office, is not a release of personal information under this part. The sheer volume of such transfers make it difficult or impossible to identify readily specific individual records.

(3) When disposing of or destroying large quantities of records containing personal information, care must be exercised to ensure that the bulk of the records is maintained so as to prevent specific records from being readily identified. If bulk is maintained, no special procedures are required. If bulk cannot be maintained or if the form of the records make individually identifiable information easily available, dispose of the record in accordance with paragraph (c)(1) of this section.

Subpart C—Collecting Personal Information

§ 310.20 General considerations.

(a) *Collect directly from the individual.* Collect to the greatest extent practicable personal information directly from the individual to whom it pertains if the information may be used in making any determination about the rights, privileges, or benefits of the individual under any federal program (see also paragraph (c) of this section).

(b) *Collecting Social Security Numbers (SSNs).* (1) It is unlawful for any federal, state, or local governmental agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, if a federal statute requires that the SSN be furnished or if the SSN is required to verify the identity of the individual in a system of records that was established and in use before January 1, 1975, and the SSN was required as an identifier by a statute or regulation adopted before that date, this restriction does not apply.

(2) When an individual is requested to provide his or her SSN, he or she must be advised:

(i) The uses that will be made of the SSN;

(ii) The statute, regulation, or rule authorizing the solicitation of the SSN; and

(iii) Whether providing the SSN is voluntary or mandatory.

(3) Include in any systems notice for any system of records that contains SSNs a statement indicating the authority for maintaining the SSN and the sources of the SSNs in the system. If the SSN is obtained directly from the individual indicate whether this is voluntary or mandatory.

(4) Executive Order 9397, "Numbering System For Federal Accounts Relating to Individual Persons," November 30, 1943, authorizes solicitation and use of SSNs as numerical identifier for individuals in most Federal records systems. However, it does not provide *mandatory* authority for soliciting SSNs.

(5) Upon entrance into military service or civilian employment with the Department of Defense, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. Provide the notification in paragraph (b)(2) of this section to the individual when originally soliciting his or her SSN. After an individual has provided his or her SSN for the purpose of establishing a record, the notification in paragraph (b)(2) is not required if the individual is only requested to furnish or verify the SSNs for identification purposes in connection with the normal use of his or her records. However, if the SSN is to be written down and retained for any purpose by the requesting official, the individual must be provided the notification required by paragraph (b)(2) of this section.

(6) Consult the Office of Personnel Management, Federal Personnel Manual (5 CFR parts 293, 294, 297 and 735) when soliciting SSNs for use in OPM records systems.

(c) *Collecting personal information from third parties.* It may not be practical to collect personal information directly from the individual in all cases. Some examples of this are:

(1) Verification of information through third party sources for security or employment suitability determinations;

(2) Seeking third party opinions such as supervisory comments as to job knowledge, duty performance, or other opinion-type evaluations;

(3) When obtaining the needed information directly from the individual is exceptionally difficult or may result in unreasonable costs; or

(4) Contacting a third party at the request of the individual to furnish certain information such as exact periods of employment, termination dates, copies of records, or similar information.

(d) *Privacy Act Statements.* (1) When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement is required regardless of the medium used to collect the information (forms, personal interviews, stylized formats, telephonic interviews, or other methods). The Privacy Act Statement consists of the elements set forth in paragraph (d)(2) of this section. The statement enables the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement need not be given. However, personal information obtained without a Privacy Act Statement shall not be incorporated into any system of records. When soliciting SSNs for any purpose, see paragraph (b)(2) of this section.

(2) The Privacy Act Statement shall include:

(i) The specific federal statute or Executive Order that authorizes collection of the requested information (see paragraph (d) of § 310.10).

(ii) The principal purpose or purposes for which the information is to be used;

(iii) The routine uses that will be made of the information (see § 310.41(e), subpart E);

(iv) Whether providing the information is voluntary or mandatory (see paragraph (e) of this section); and

(v) The effects on the individual if he or she chooses not to provide the requested information.

(3) The Privacy Act Statement shall be concise, current, and easily understood.

(4) The Privacy Act statement may appear as a public notice (sign or poster), conspicuously displayed in the area where the information is collected, such as at check-cashing facilities or identification photograph facilities.

(5) The individual normally is not required to sign the Privacy Act Statement.

(6) Provide the individual a written copy of the Privacy Act Statement upon request. This must be done regardless of the method chosen to furnish the initial advisement.

(e) *Mandatory as opposed to voluntary disclosures.* Include in the Privacy Act Statement specifically whether furnishing the requested personal data is mandatory or voluntary. A requirement to furnish personal data is mandatory only when a federal statute, Executive Order, regulation, or other lawful order specifically imposes a duty on the individual to provide the information sought, and the individual is subject to a penalty if he or she fails to provide the requested information. If providing the information is only a condition of or prerequisite to granting a benefit or privilege and the individual has the option of requesting the benefit or privilege, providing the information is always voluntary. However, the loss or denial of the privilege, benefit, or entitlement sought may be listed as a consequence of not furnishing the requested information.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57800, Nov. 14, 1991]

§ 310.21 Forms.

(a) *DoD forms.* (1) DoD Directive 5000.21, "Forms Management Program" provides guidance for preparing Privacy Act Statements for use with forms (see also paragraph (b)(1) of this section).

(2) When forms are used to collect personal information, the Privacy Act Statement shall appear as follows (listed in the order of preference):

(i) In the body of the form, preferably just below the title so that the reader will be advised of the contents of the